

Secure Mobile Cloud Computing for Sensitive Data: Teacher Services for Palestinian Higher Education Institutions

Mahmoud M. Abu Ghosh¹, Rasha R. Atallah², and Samy S. Abu Naser³

^{1,2}Faculty of Information Technology,
University of Palestine, Gaza, Palestine

³ Faculty of Engineering & Information Technology,
Al-Azhar University, Gaza, Palestine

¹ma.abughosh@gmail.com, ²r.attallah@up.edu.ps, ³sabunaser@gmail.com

Abstract

Many Palestinian higher education institutions had a successful experience in utilizing Electronic Services and Electronic learning, such as all the academic services for student and lecturer, schedule lectures, exams schedule, viewing the academic information, grades report, printing transcript, registering courses, library services, Email services, News and Announcements, but these services are supported by web based applications or desktop application which restrict the access of the users using computers or laptops, But there is a lack in supporting these services with mobile. Especially when dealing with sensitive data as inserting grades for courses. So in this paper we present a system called Secure Mobile Cloud Computing for Sensitive Data: Teacher Services for Palestinian Higher Education Institutions (MCCTSs) which is a mobile application to facilities access using RSA algorithm to encrypt the data which sent and received through Cloud computing application. MCCTSs serve the lecturers of Palestinian higher education institutions. Agile methodology was adapted to develop MCCTSs application. MCCTSs users successfully insert the grades securely and encrypted any time anywhere using RSA algorithm. It is hoped that the result of this study will encourage the universities to engage MCCTSs in their services. From the results we obtained, it is proved that RSA provides protection for the data, which is stored in Cloud. Only authorized user can read the encrypted data and decrypt it. Even if anyone happens to read the data accidentally, the original meaning of the data will not be understood.

Keywords: Higher Education, Electronic Learning, Cloud Computing, RSA, Mobile

1. Introduction

Many Palestinian higher education institutions had a successful experience in utilizing Electronic Services and Electronic learning. Most of University services are currently applied as an electronic web application.

Services such as lecture inserting grades, schedule, exams schedule, viewing the academic information, grades report, library services, Email services, eLearning services, News and Announcements, but these services are only supported by web based applications or desktop application which restrict the access of the users using computers or laptops.

Users need to access the University services anytime and anywhere as mobile services, and need to insert sensitive data, so in this paper we present a system called Secure Mobile Cloud Computing for sensitive data: Teacher Services for Palestinian Higher Education Institutions (MCCTSs) which is a mobile application to facilities access using RSA algorithm, to encrypted the data to be send and received through Cloud computing application. MCCTSs serve the lecturers of Palestinian higher education institutions.

According to a study we have done, there is a strong evidence on the readiness of academic staff to accept and use Academic Services on Mobile in their education environment.

2. Technical Fundamental

2.1 Cloud Computing

Cloud computing is on-demand computing that does not reside at the user's premise (Instead, the computing resources (*e.g.*, networks, servers, storage, services) are owned and managed by a service provider and the users access the resources via the internet. Cloud computing is web-based processing, shared resources and information provided on demand to portable devices and computers to the users for processing [1, 5].

2.2 Benefits of Cloud Computing

The most important benefits of Cloud Computing is saving money and time [2, 3, 4, 6].

1. **Reduced Cost:** Cloud Computing reduces overall physical hardware and maintenance of these hardware [7]. Only pay for what use from the Cloud Computing resource pool.
2. **Scalability of System:** Can easily request for more processing power from the resource pool at very minimum cost according to the user requirement.
3. **Automatic Updates of Software:** Cloud Computing company will automatically update the software if a new version is released.
4. **Remote Access of the System:** The user can access the data from anywhere around the world.
5. **Disaster Relief:** The Cloud Computing Company keeps the backup of data and ensures the proper functioning of the system.
6. **Quick Customer Support:** the Cloud Computing vendor provides quick customer support, which is essential for the functioning of the business.
7. **Sufficient Storage:** more space is available for storage of the data
8. **Service Models:** Cloud computing providers offer their services according to several fundamental models:
 - **Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure [13]. The applications are accessible from various client devices through a thin client interface such as a web browser (*e.g.*, web-based email).
 - **Platform as a Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer created or acquired applications created using programming languages and tools supported by the provider.
 - **Infrastructure as a Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

2.3 Data Security Issues in Cloud Computing

- **Privacy and Confidentiality:** Once the client show data to the cloud there should be some security that access to that data will only be incomplete to the authorized access. Inappropriate access to client sensitive data by cloud staff is another risk that can create potential threat to cloud data. The client is being provided assurance and proper practices and safe policies and procedures should be in place to guarantee the

cloud users of the data safety. The cloud seeker must be assured that data propagate on the cloud will be confidential [5].

- **Data Integrity:** With getting the security of data, cloud service providers should apply mechanisms to ensure data truthfulness and be able to tell what happened to a definite data set and at what point. The client should be aware by the data provider the origin and the integrity mechanisms put in place.
- **Data Location and Relocation:** Cloud computing offers a high amount of data mobility. Consumers do not always know location of their data. However, when an venture has some sensitive data that's reserved over a storage device in the Cloud, they will often keep asking the career than it. They will also aspiration to specify a chosen location (*e.g.* data being trapped in India). This, then, needs a contractual agreement, between your Cloud provider and also the consumer that data should live in a certain location or reside on a given known server. Also, cloud providers should take accountability to guarantee the security of systems (including data) and gives robust certification to protect customer's information.
- **Data Availability:** Customer info is normally saved in chunk on different servers often residing in different locations or even in different Clouds. In such cases, data availability becomes a major legitimate issue because use of un-interruptible and seamless provision becomes relatively difficult.

2.4 Security Disadvantages in Cloud Environment

Data Segregation: Data in the cloud is usually in a shared environment together with data from other clients. Encryption cannot be understood as the single solution for data separation problems. In some situations, customers would not like to encrypt data because there can be a case when encryption accident can demolish the data.

2.5 RSA Algorithm

RSA algorithm is public key encryption. This algorithm is brought to life by Ron Rivest, Adi Shamir and Len Adelman in 1977. It is strong asymmetric key cryptographic algorithm. It may well used to provide secrecy. Therein algorithm uses the top number to come up with people key and key depending on mathematical fact and multiplying huge numbers together. It uses the block size data during which plain-text and cipher text are integers between 0 and n for a lot of n values. Size n is known as 1024 bits [7, 8, 9].

3. Related Work

Uma Somani *et al.* (2010) in implementing the Digital Signature with RSA Encryption Algorithm to Boost the Data Security of Cloud in Cloud Computing [20] have described the cloud storage methodology and proposed algorithm and Implementing the RSA algorithm through Digital Signature. And proposed the gradually process consumed in Digital Signature with RSA algorithm. If these implementing algorithms are combined in other encryption techniques (*i.e.* DES, AES *etc*) then it's became stronger and secure for cloud computing [8].

Abu Naser *et al.* (2013) Implementing Mobile Cloud Computing Academic Services at Palestinian Higher Education Institutions (MCCAS), which is a mobile application to facilitate access. MCCAS serve the students and the academic staff of Palestinian higher education institutions. According to a study we have done, there is a strong evidence on the readiness of academic staff and students to accept and use Academic Services on Mobile in their education environment. A survey was carried out on a group of academic staff and students who used MCCAS application and answered the survey questions. The survey answered by 220 students and 51 academic staff with different levels, gender and different types of phones. The survey emphasized that MCCAS satisfies academic staff

and student needs and run with high performance and compatible with all OS devices and achieved the main objective of our system [10]

4. Secure Mobile Cloud Computing for Sensitive Data: Teacher Services for Palestinian Higher Education Institutions

Our proposed model is a mobile application for helping academic staff in higher education institutions to insert the sensitive data as marks in secure way anywhere and anytime. Our application can deal with android, IOS, and windows phone, the system supports the Arabic and English language. Figure 1 show the mechanism of MCCTSs.

4.1 The Mechanism of MCCTSs:

The teacher open the application using his username and password using GOOGLE cloud computing to connect to Registration Database of the Universities and used, also the application used HTTPs.

MCCTSs use RSA algorithm to encrypt the sensitive data as the marks to transmit to the data base.

The server of Database decrypts the data and stores them on the Database, so RSA guarantee that the data not changed or hacked.

The process of retrieve the sensitive data does not need to be encrypt, as the process of view the grades.

4.2 The Analysis of Security

The security analysis done based on preventing some attacks. Brute Force Attack: Prevent the decryption of any message using RSA to encrypt it , So it is difficult to guess the key.

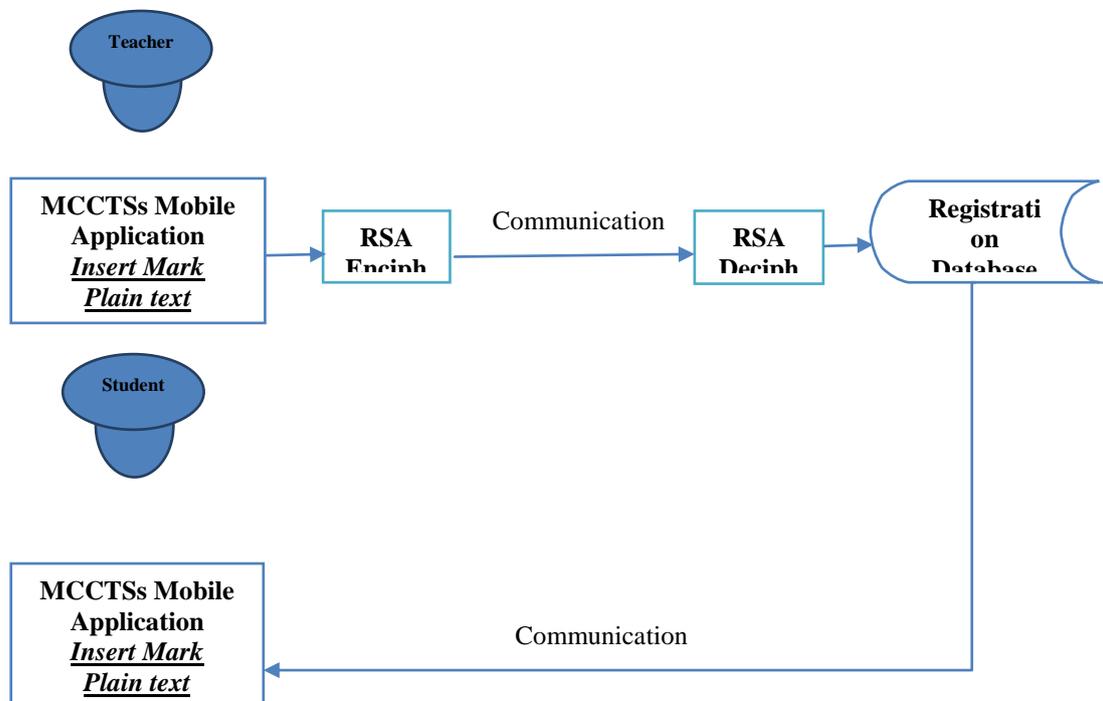


Figure 1. Shows the Mechanism of MCCTS

5. Conclusion

In this paper we presented a system called Secure Mobile Cloud Computing for Sensitive Data: Teacher Services for Palestinian Higher Education Institutions (MCCTSs) which is a mobile application to facilities access using RSA algorithm to encrypt the data which sent and received through Cloud Computing application. MCCTSs serve the lecturers of Palestinian higher education institutions. Agile methodology was used to develop MCCTSs application. MCCTSs users successfully inserted the grades securely and encrypted all the time anywhere using RSA algorithm. It is hoped that the outcome of this study will encourage the universities to engage MCCTSs in their services. From the results we obtained, it is proved that RSA provides protection for the data, which is stored in Cloud. Only authorized user can read the encrypted data and decrypt it.

References

- [1] T. Hoang Dinh. *et al* "A survey of mobile cloud computing, architecture, application and approaches". <http://onlinelibrary.wiley.com/doi/10.1002/wcm.1203/full>, (2011).
- [2] M. Papazoglou, "Web Services Technologies and Standards", Computing Surveys, (2006), pp. 1-41.
- [3] G. Abdulsalam & Fatima, Z, "Cloud Computing: Solution to ICT in Higher Education in Nigeria", Pelagia Research Library Communications of the ACM, vol. 51, (2011) pp. 9-11.
- [4] D. White, " Cloud Computing: The Risks, Benefits, and Success Factors"[Retrieved March 5,2013] <http://cloudcomputing.syscon.com/node/1924251>, (2011).
- [5] D. C Wyld, "Cloud Computing 101: Universities are Migrating to The Cloud for Functionality and Savings," Computer Sight. [Online], [Retrieved October 5,2010], <http://computersight.com/programming/cloudcomputing-101-universities-aremigrating-to-the-cloud-for-functionalityand-saving/>, (2009).
- [6] D. C Wyld, "Cloud Computing 101: Universities are Migrating to The Cloud for Functionality and Savings," Computer Sight. [Online]. <http://computersight.com/programming/cloudcomputing-101-universities-aremigrating-to-the-cloud-for-functionalityand-saving/>, (2009).
- [7] P. Riikonen, "RSA Algorithm", (2002).
- [8] U. Somani, K. Lakhani, M. Mundra, "Implementing Digital Signature with RSA Encryption to Enhance Data Security of Cloud in Cloud Computing", IEEE, (2010).
- [9] P. Prasad, B. Ojha, R. Ranjan shahi, R. Lal, "3 Dimensional Security in Cloud Computing", IEEE, (2011).
- [10] S. Abu Naser , M. Abu Ghosh , R. Atallah, "Mobile Cloud Computing: Academic Services for Palestinian Higher Education Institutions (MCCAS)", International Journal of Research in Engineering and Science (IJRES) ISSN (Online): 2320-9364, ISSN (Print): 2320-9356 , www.ijres.org, vol. 3, issue 1, (2015) pp.22-27.
- [11] Prof. S. S. Abu Naser, M. Abu Ghosh, and R. R. Atallah, "Using Social network in Higher Education acase Study on the University of Palestine", IJERA, (2014).
- [12] R. R. Atallah, Professor S. S. Abu Naser, Data Mining Techniques in Higher Education an Empirical Study for theUniversity of Palestine,IJMER, vol. 4, no. 4 , (2014), pp. 48-52.
- [13] Prof. S. S. Abu Naser, R. R. Atallah, S. Hamo, "Building an Ontology in Educational Domain Case Study for the University of Palestine", International Journal of Research in Engineering and Science (IJRES), vol. 3, no. 1, (2015).

